Kurdish Studies
Jan 2024
Volume: 12, No: 1, pp. 3426-3454
ISSN: 2051-4883 (Print) | ISSN 2051-4891 (Online)
www.KurdishStudies.net

Received: October 2023 Accepted: December 2023
DOI: https://doi.org/10.58262/ks.v12i1.242

Securing the Evolving Iot with Deep Learning: A Comprehensive Review

Usman Tariq [1*], Irfan Ahmed[2], Ali Kashif Bashir [3], Muhammad Attique Khan[4]

Abstract

This paper explores how deep learning enhances Internet of Things (IoT) cybersecurity, examining advanced methods like convolutional and recurrent neural networks for detailed IoT data analysis. It highlights the importance of real-time threat detection and classification, focusing on innovative Graph Neural Networks and Transformer Models for better network security. The study also considers Federated Learning and Edge Computing for decentralized, privacy-friendly data handling, and Explainable AI for clarity in decision-making. It addresses the growing challenges of creating scalable, adaptable deep learning models for ever-changing IoT environments and cyber threats, emphasizing the need for ongoing research in developing resilient IoT cybersecurity solutions. The analysis further reveals that deep learning techniques are increasingly effective in anomaly detection and predictive maintenance, reducing false positives, and adapting to new types of cyber threats dynamically. Specifically, it emphasizes how Transformer Models and Graph Neural Networks offer promising results in contextualizing and mitigating complex multi-stage cyber-attacks, enhancing the robustness of IoT systems against evolving threats.

Keywords: *Pervasive IoT systems; Intelligent anomaly detection cybersecurity challenges; Anomaly diagnosis; Deep Learning algorithms; Estimation correlation.*

Introduction

The IoT represents a transformative shift in the digital landscape, marking the evolution of the internet from a network of computers to a network of connected nodes. These devices, ranging from everyday house-hold items to sophisticated industrial tools, are embedded with sensors, software, and other technologies, enabling them to accumulate and exchange data. This interconnectedness allows for a level of digital intelligence in objects that were previously inert, enabling them to communicate re-al-time data without requiring human intervention. The concept of IoT, which emerged in the late 1990s, has evolved dramatically over the years. The early stages of IoT were marked by introducing RFID tags and the proliferation of wireless technologies. Over time, advancements in sensor technology, cloud computing, and machine learning have propelled IoT from a nascent idea to a central component of the modern digital ecosystem (Tang, 2023).

[1] Department of Management Information Systems, College of Business Administration, Prince Sattam Bin Abdulaziz University, Al-Kharj 16278, Saudi Arabia, Email: u.tariq@psau.edu.sa,Tel: (+966115887080)
[2] Department of Computer Science, College of Engineering, Virginia Commonwealth University, Richmond, VA – 23284, USA
Email: iahmed3@vcu.edu
[3] Department of Computing and Mathematics, Manchester Metropolitan University, Manchester M156BH, UK, Email: a.bashir@mmu.ac.uk
[4] Department of Computer Science, HITEC University, Taxila, Pakistan, Email: attique@ciitwah.edu.pk

IoT's influence extends across various sectors, revolutionizing traditional practices and introducing un-precedented efficiency and innovation (Hassebo & Tealab, 2023). In healthcare, for in-stance, IoT-enabled devices like wearable fitness trackers and remote patient monitoring systems offer insights into patient health outside of traditional clinical settings. Agriculture has seen a surge in precision farming techniques, where IoT de-vices pro-vide real-time information on soil conditions, crop health, and livestock, leading to in-formed decisions and increased productivity. Smart cities leverage IoT for optimized traffic management, enhanced public safety, and sustainable energy usage. Manufacturing benefits from IoT through predictive maintenance and streamlined supply chains, while home automation systems afford convenience and energy efficiency. Each of these sectors demonstrates the versatility of IoT applications, highlighting its capacity to transform everyday operations into da-ta-driven, intelligent processes.

Despite its numerous benefits, IoT is not without its challenges (H.J. & S., 2022). Security and privacy concerns are at the forefront, with the increase in connected devices creating more entry points for cyberattacks and data breaches. The complexity and scale of IoT networks also pose challenges in ensuring data privacy and protection. Moreover, the integration of IoT systems requires significant investment in infrastructure and skills development. Looking ahead, the future of IoT is intertwined with advancements in technologies like 5G, edge computing, and artificial intelligence. These technologies are expected to further enhance the capabilities of IoT systems, making them more efficient, secure, and intelligent. As IoT continues to evolve, it stands as a testament to human ingenuity, with the potential to further revolutionize industries, catalyze in-novation, and reshape how we interact with the world around us.

Table 1 Breakdown of Publication Years in Analyzed Research Papers (Derived from Google Scholar Search Data)

Year	Published (# of research papers)	Our Investigation (# of research papers)
2023	38,800	1552
2022	40,600	1624
2021	35,300	1412
2020	20,800	624
2019	12,100	242

Table 2 Evaluation of Key Terms in Principal Research Studies.

Keywords	Count	Keywords	Count
Deep Learning			
Neural Networks	953	Convolutional Neural Networks (CNN)	897
Recurrent Neural Networks (RNN)	600	Deep Reinforcement Learning	465
Backpropagation	693	Long Short-Term Memory (LSTM)	667
Generative Adversarial Networks (GAN)	650	Autoencoders	397
Transfer Learning	500	Feature Extraction	714
Activation Functions	261	Dropout Regularization	192
Gradient Descent	800	Supervised Learning	750
Unsupervised Learning	549	Deep Belief Network	194
Overfitting	355	Data Augmentation	291
Loss Functions	385	Tensor Processing Units (TPU)	148
Adam Optimizer	221	Hyperparameter Tuning	396
Batch Normalization	445	Attention Mechanisms	497
Feedforward Neural Networks	499	Boltzmann Machines	197
Dropout Techniques	284	Gradient Descent Algorithms	551
Sequence Modeling	314	Graph Neural Networks (GNNs)	499

Keywords	Count	Keywords	Count
Internet of Things (IoT)			
Edge Computing	674	Internet of Things (IoT)	1001
IoT Security	947	IoT Protocols	367
IoT Devices	781	Blockchain in IoT	381
Smart Grids	498	Smart Cities	652
Smart Healthcare	552	Predictive Maintenance	475
Machine-to-Machine Communication	556	Cloud Computing	821
Sensor Networks	577	Energy Harvesting for IoT	250
IoT Standards	582	IoT and Artificial Intelligence	743
Fog Computing	442	IoT Privacy Issues	574
Cybersecurity			
Network Security	889	Cyber Threats	958
Data Breaches	791	Encryption	738
Authentication	697	Authorization	371
Anomaly Detection	598	Intrusion Detection Systems (IDS)	700
Botnet Attacks	554	DDoS Attacks	581
Malware	847	Vulnerability Assessment	541
Cybersecurity Frameworks	519	Ethical Hacking	388
Machine Learning (as it relates to cybersecurity applications)	753	IoT Ransomware	257
IoT Spoofing Attacks	287	IoT Cybersecurity Frameworks	350
Penetration Testing	659	GDPR Compliance	447

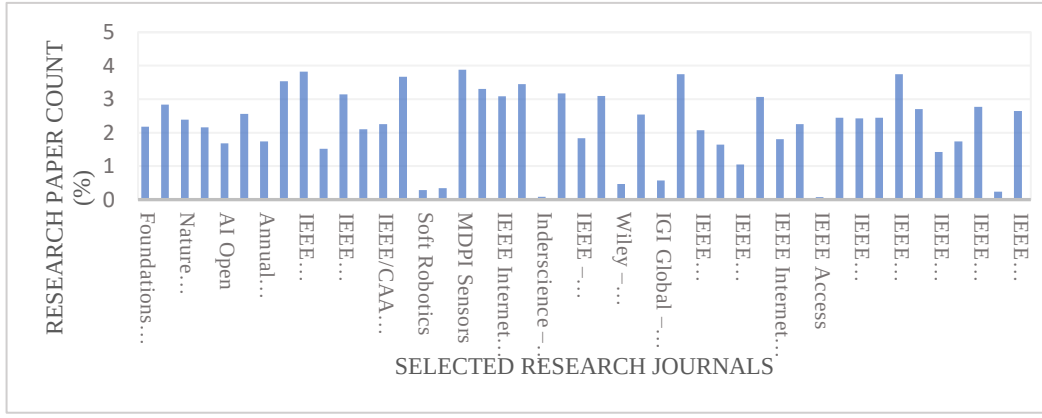

Figure1: Research Dispersal and Distribution Statistics.

Considering the data presented in Table 1, Table 2, and Figure 1, it's evident that choosing an appropriate journal and keywords is vital for research in 'Deep Learning based IoT Cybersecurity'. Selecting the right journal aligns the research with a suitable audience and enhances its impact, which is particularly essential in a dynamic and multidisciplinary domain like this. Meanwhile, careful keyword selection boosts the research's visibility in academic databases, encouraging engagement from peers and experts in the field. This methodical approach not only broadens the re-search's reach but also encourages collaborative progress in the innovative intersection of deep learning and IoT cybersecurity.

The main contributions of the projected review paper are as follows

a) The paper offers an in-depth examination of various deep learning techniques and their application in enhancing IoT cybersecurity. It delves into the effectiveness of different DL models, including CNNs, RNNs, GNNs, and Transformer Models, in identifying and mitigating cyber hazards in IoT environments.

b) It evaluates advanced deep learning architectures and their appropriate-ness for complex IoT security challenges, providing insights into how these models can be optimized for better performance in IoT contexts.
c) The paper discusses the integration of Federated Learning and Edge Computing in IoT cybersecurity. This includes leveraging these technologies for decentralized, efficient, and privacy-preserving data processing in IoT networks.
d) There is a focus on the importance and application of Explainable AI (XAI) in the context of IoT cybersecurity, emphasizing the need for transparency and understandability in DL-driven security solutions.
e) The paper identifies and discusses future research directions, including the development of lightweight DL models for resource-constrained IoT devices, and the need for DL models to adapt to dynamic IoT environments and emerging cyber threats.
f) It highlights ongoing challenges and open questions in applying DL to IoT cybersecurity, such as issues related to data privacy, model explainability, and computational efficiency.

Following the Introduction section, the research paper's narrative unfolds in a structured manner. Initially, it probes into the complexities of DL within IoT cybersecurity, covering a range of DL models such as CNNs, RNNs, and their sophisticated variations. The focus is on adapting these models to the specific needs of IoT settings, with special attention to malware detection and processing sequential data. Subsequently, the pa-per ventures into the realm of GNNs and Transformer Models, shedding light on their vital role in the intricate network analyses essential for securing IoT systems. An in-depth analysis of Federated Learning and Edge Computing follows, highlighting their significance in facilitating decentralized and privacy-focused data processing. Moreover, the paper touches upon the role of Explainable AI in the domain of IoT cybersecurity, stressing the need for DL solutions that are both transparent and comprehensible. The paper wraps up with a forward-looking discussion on potential avenues for future research, pinpointing essential areas like developing resource-efficient DL models suitable for IoT devices, and the need for DL approaches to evolve in response to the changing dynamics of IoT environments and new cybersecurity threats. Throughout, the paper keeps its lens trained on the advanced deployment of DL to bolster IoT cybersecurity, aiming to offer an exhaustive and perceptive overview of this rapidly progressing field.

Deep Learning in Iot

Deep learning, a subset of machine learning, stands at the forefront of the techno-logical revolution, particularly in its synergy with the Internet of Things. At its core, deep learning relies on neural networks, which are encouraged by the human brain's configuration and function. These systems are comprised of layers of interrelated nodes or 'neurons' that process data hierarchically. Among the various architectures, Convolutional Neural Networks (Ghorsad & Zade, 2023) are renowned for their proficiency in handling visual data, making them ideal for image and video analysis. Recurrent Neural Networks (Ahn & Park, 2021), on the other hand, excel in processing sequential data, which is crucial for time-series analysis or natural language processing. These architectures enable machines to extract pat-terns and learn from vast amounts of data, a capability especially pertinent in the IoT domain, where devices generate and communicate a continuous stream of information.

The convergence of deep learning and IoT is reshaping how we interact with technology, making IoT de-vices not just data collectors but intelligent analysts and decision-makers (Yan et al., 2022). For instance, deep learning algorithms in healthcare process data from IoT devices

like wearable health monitors, enabling real-time health status assessments and early disease detection. In industrial automation, DL-driven IoT systems predict equipment failures, optimizing maintenance schedules and reducing down-time. Smart cities bene-fit too, with deep learning enhancing IoT applications in traffic management, environmental monitoring, and public safety, leading to smarter, more efficient urban living. These applications underscore how deep learning augments IoT's capability, transforming raw data into actionable insights, thereby enhancing efficiency, predictive accuracy, and user experience.

Investigating specific case studies illustrates this transformative impact. In one instance, a manufacturing plant integrated deep learning algorithms with its IoT net-work to predict machine failures, significantly reducing unplanned downtime and maintenance costs (Murugiah et al., 2023). Another case saw a smart city initiative leverage deep learning powered IoT devices to analyze traffic patterns, improving congestion management and reducing pollution (Damadam et al., 2022). These examples highlight the challenges - like managing complex datasets and ensuring real-time processing - and the innovative solutions deep learning provides, leading to substantial improvements in operations and service delivery. Thereby, deep learning's role in advancing IoT is un-deniable, offering smart-er, more efficient, and responsive solutions. As technology progresses, the future will likely see even deeper integration of these fields, with emerging trends like edge computing and federated learning opening new possibilities for IoT applications enhanced by deep learning.

Table 3 Comparative Overview of Deep Learning Models for IoT Cybersecurity: Applications, Relevant Datasets, and Key Evaluation Metrics.

Ref.	Methodology	Deep Learning Model	Dataset Name	Evaluation Metrics
(Audibert, Michiardi, et al., 2022)	Anomaly Detection in IoT Devices	CNNs	IoT-23 (Sudhakar & Senthilkumar, 2023)	Accuracy, F1 Score
(Michiardi, et al., 2020)	Intrusion Detection System (IDS)	RNNs	KDD Cup 99 Choudhary & Kesswani, 2020)	Precision, Recall
(Han, et al., 2022)	Network Traffic Analysis	LSTMs	UNSW-NB15 (Yoon & Hwang, 2021)	Area Under Curve (AUC)
(Catillo, et al., 2023)	User Behavior Analytics	Autoencoders	N-BaIoT (Meidan et al., 2018)	Mean Squared Error (MSE)
(Gordon, 2023)	Malware Detection	GANs	Malware IoT Dataset	Detection Rate
(Wang et al., 2022)	IoT Device Classification	DBNs	IoT Device Fingerprinting	Accuracy, Precision
(Moro, et al., 2023)	Energy Consumption Modeling	RBMs	Smart Home Dataset	Root Mean Square Error (RMSE)
(Kholidy, 2020)	Time Series Prediction in IoT	Sequence-to-Sequence Models	IoT Time Series Dataset	Mean Absolute Error (MAE)
(Ali, et al., 2021)	Privacy-Preserving Data Analysis	VAEs	Private IoT Dataset	KL Divergence
(Demirkıran, et al., 2022)	Traffic Flow Prediction	Transformer Models	Urban IoT Dataset	Mean Squared Logarithmic Error (MSLE)
(Ilango, Ma, & Su, 2022)	Sensor Data Fusion	Feedforward Neural Networks	Multi-Sensor IoT Dataset	Correlation Coefficient

Ref.	Methodology	Deep Learning Model	Dataset Name	Evaluation Metrics
(Kamala & Nawaz, 2023)	Smart Grid Anomaly Detection	Multi-Layer Perceptrons (MLPs)	Electricity IoT Dataset	Precision, Recall
(Wang et al., 2023)	Biometric Authentication	Bidirectional Long Short-Term Memory Networks (BiLSTMs)	Biometric IoT Dataset	Equal Error Rate (EER)
(Iliyasu & Deng, 2020)	Fake IoT Device Detection	Deep Convolutional Generative Adversarial Networks (DCGANs)	IoT GAN Dataset	F1 Score, Accuracy
(Cheng, Xu, Li, & Han, 2022)	Smart City Surveillance	Attention Mechanism Models	City Surveillance Dataset	Recall, Precision
(Wu, Dai, & Tang, 2022)	Structural Health Monitoring	GNNs	Infrastructure IoT Dataset	RMSE, MAE
(Sellami, Hakiri, & Ben Yahia, 2022)	Autonomous IoT Systems	Deep Reinforcement Learning Models	Autonomous IoT Dataset	Reward Efficiency
(Yao et al., 2019)	3D Object Recognition in IoT	Capsule Networks	3D IoT Object Dataset	Accuracy, Precision
(Khan & Mailewa, 2023)	Network Topology Analysis	Self-Organizing Maps (SOMs)	IoT Topology Dataset	Topological Error
(Zhu, Jang-Jaccard, & Watters, 2020)	IoT Device Authentication	Siamese Neural Networks	IoT Authentication Dataset	Accuracy, EER

In Table 3, the 'Methodology' column specifies the particular cybersecurity task or challenge being tackled, focusing on issues pertinent to the IoT environments. The 'Dataset Name' refers to carefully curated datasets that are optimally suited for both training and evaluating deep learning models within the sphere of IoT cybersecurity. These datasets were designed to encapsulate characteristics and threats unique to IoT systems. The 'Evaluation Metrics' section details the criteria used for measuring the efficacy of the deep learning models. Depending on the nature of the task - whether it's classification or regression - different metrics were employed, such as accuracy, precision, recall, and F1 score for classification, or mean squared error for regression-based tasks. This structured approach ensures a focused and relevant assessment of deep learning models in addressing cybersecurity challenges in IoT contexts.

Cybersecurity Challenges in Iot

In the trajectory of IoT cybersecurity, the landscape is constantly evolving, with a variety of threats and vulnerabilities posing significant challenges. Common threats include Distributed Denial of Service (DDoS) attacks (Almaraz-Rivera et al., 2023), which devastate IoT net-works, rendering them inoperable; malware (Wu, et al., 2023), which can covertly infiltrate and com-promise devices; and data breaches, where sensitive information is illicitly accessed or stolen. Each attack exploits specific weaknesses in IoT systems, such as inadequate authentication, unencrypted data transmission, and lack of regular software updates. The examination of notable case studies, like the Mirai botnet attack (Yusuf et al., 2023) which harnessed thousands of compromised IoT devices, reveals the multifaceted nature of these threats. Such analyses

not only shed light on the methods employed by attackers but also on the profound impact on affected systems, thereby underscoring the vital lessons for enhancing IoT security.

Addressing these concerns requires a robust approach to risk mitigation, encompassing a spectrum of strategies and security frameworks. Effective risk management in IoT involves implementing layered security measures, including advanced encryption methods for data-in-transit and at-rest, rigorous device authentication protocols, and continuous network monitoring for anomaly detection. Security frameworks like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (Puteho et al., 2023, 2023) provide structured guidance for managing and reducing cybersecurity risk in IoT contexts. Moreover, it is essential to follow established IoT security protocols and standards. These include the Transport Layer Security (TLS) for safe data transmission and the Open Web Application Security Project (OWASP) IoT Top Ten (Riandhanu, 2022), which helps in spotting and thwarting prevalent IoT vulnerabilities. Nonetheless, the swift advancement of IoT technology and the ever-changing setting of cyber threats call for continuous review and modification of these standards. This indicates a fluid and evolving future for IoT security protocols and frameworks.

Table 4 A comparative analysis of IoT Protocols and their Security Services (Tariq, et al., 2023), (Naeem et al., 2023), (Tariq, et al., 2023).Available (✓) , Not Available (X).

Protocol/Service	Privacy Service (Confidentiality)	Access Control Service (Authorization)	Identity Verification Service (Authentication)	Ciphering Service (Encryption)
Simple Service Discovery Protocol (SSDP)	X	X	X	X
Multicast Domain Name System (mDNS)	X	X	X	X
Extensible Messaging and Presence Protocol (XMPP)	✓	✓	✓	✓
Data Distribution Service (DDS)	✓	✓	✓	✓
Advanced Message Queuing Protocol (AMQP)	✓	✓	✓	✓
Constrained Application Protocol (CoAP)	✓	✓	✓	✓
Message Queuing Telemetry Transport (MQTT)	✓	✓	✓	✓
HTTP/HTTPS	✓ (HTTPS)	✓	✓	✓ (HTTPS)
WebSocket	✓	✓	✓	✓
Lightweight M2M	✓	✓	✓	✓
Zigbee	✓	✓	✓	✓
Z-Wave	✓	✓	✓	✓
Long Range Wide Area Network (LoRaWAN)	✓	✓	✓	✓
IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN)	✓	✓	✓	✓
BLE (Bluetooth Low Energy)	✓	✓	✓	✓
Near Field Communication (NFC)	✓	✓	✓	✓
Radio Frequency Identification (RFID)	✓	✓	✓	✓
Modbus	X	X	X	X
Building Automation Control Network (BACne)t	✓	✓	✓	✓
Konnex (KNX)	✓	✓	✓	✓

Table 4 highlights the varying degrees of cybersecurity services offered by different IoT protocols. Protocols like XMPP, DDS, AMQP, CoAP, MQTT, and others such as HTTP/HTTPS, WebSocket, and LwM2M provide comprehensive security services covering confidentiality, authorization, authentication, and encryption. In contrast, protocols like SSDP and mDNS do not inherently offer these security services. It's essential to note that the availability of these services can be dependent on the implementation and configuration of the protocol within the IoT ecosystem.

Deep Learning for Iot Security

Deep learning models have significantly enhanced the capabilities of Intrusion Detection Systems (IDS) (Ahanger et al., 2020)] in the realm of IoT security. For instance, CNNs excel in feature extraction from high-dimensional data, making them suitable for analyzing network traffic patterns and identifying malicious activities (Aversano et al., 2021). RNNs, particularly effective in sequential data analysis, are used to monitor time-series data from IoT de-vices, thus detecting anomalies over time. GNNs are adept at modeling network traffic as graphs, providing a holistic view of interconnect-ed IoT devices and identifying potential threats based on network topology (Yumlembam et al., 2023).

Deep Belief Networks (DBNs) and Restricted Boltzmann Machines (RBMs) are instrumental in unsupervised learning scenarios, uncovering hidden patterns in IoT data without labeled examples. This feature is especially valuable in detecting zero-day at-tacks. Sequence-to-Sequence Models find application in predicting and identifying at-tack sequences, which is crucial in understanding multi-stage attack strategies. Variational Autoencoders (VAEs), known for their generative capabilities, are used in IDS to generate synthetic attack data for training purposes, enhancing the model's ability to recognize novel attack patterns (He et al., 2021)

Transformer Models, with their attention mechanisms, are proficient in handling large-scale IoT data, offering enhanced capability in identifying complex attack pat-terns that span across different devices and time frames. Feedforward Neural Net-works and Multi-Layer Perceptrons (MLPs) provide foundational deep learning structures for IDS, often serving as baseline models for performance comparison and feature learning in IoT security datasets (Qiao at al., 2021).

Table 5 Deep Learning Models in IoT Intrusion Detection Systems (Amanullah et al., 2020), (Chen et al., 2021), (Chaabouni et al., 2019), (Jahwar & Zeebaree, 2021), (Ahmad et al., 2023).

Deep Learning Model	Functions in IoT IDS	Merits	Demerits	Characteristics Helpful in IoT IDS
CNN	Traffic pattern analysis, feature extraction	High accuracy in pattern recognition	Computationally intensive	Effective in spatial data interpretation
RNN	Time-series data monitoring, sequential anomaly detection	Good at handling sequential data	Prone to vanishing gradient problem	Suitable for temporal data analysis
GNN	Network topology analysis	Effective in relational data analysis	Complex model architecture	Ideal for interconnected device data
DBN	Unsupervised anomaly detection	Efficient in uncovering hidden patterns	Training can be time-consuming	Useful in zero-day attack detection
RBM	Feature learning, pattern recognition	Good at dimensionality reduction	Sensitive to hyperparameter settings	Efficient in unsupervised learning
Sequence-to-Sequence Models	Attack sequence prediction	Good at modeling long sequences	Requires large amount of data	Useful in multi-stage attack detection
VAE	Synthetic attack data generation	Effective in generative tasks	Complexity in training and tuning	Helps in expanding training dataset
Transformer Model	Large-scale data analysis, complex pattern identification	Excellent in handling large datasets	Resource-heavy	Effective in multi-device environment
Feedforward Neural Network	Baseline model for IDS	Simplicity and ease of use	Limited in handling complex patterns	Good for initial feature learning
MLP	Feature learning, baseline performance comparison	Versatile in different data types	Prone to overfitting	Effective in foundational model building

Table 5 succinctly summarizes how each deep learning model contributes to IoT IDS. Models like CNNs and RNNs are pivotal for their respective spatial and temporal data analysis capabilities. GNNs offer a unique ad-vantage in understanding the intricate network of IoT devices. On the other hand, DBNs and RBMs excel in scenarios where labeled data is scarce. Sequence-to-Sequence models and VAEs are innovative in understanding and preparing for complex attack patterns. Transformer Models, while resource-intensive, provide unparalleled proficiency in handling extensive datasets. Traditional models like Feedforward Neural Networks and MLPs, though less complex, are crucial for foundational analyses and serve as benchmarks in the development of IDS.

Deep Learning Model's Iot Security Focused Taxonomy

Supervised Learning Models

Multilayer Perceptron's (Mlp)

In the context of IoT cybersecurity, MLPs require a well-labeled dataset with features representing network traffic characteristics. Preprocessing involves normalization and outlier removal (Firat et al., 2023). Feature engineering is crucial, often involving statistical measures of packet data. MLPs, with their deep, fully connected layers, are effective for pattern recognition in network traffic. Training involves backpropagation with hyperparameters like learning rate and epoch number tuned for optimal performance.

$$Output = f(\sum(weights \cdot inputs) + bias)$$ [eq. 1]

Here,

`Output`: The final output of the MLP, typically a class label or a continuous value.

`$f$`: Activation function, such as sigmoid, ReLU, or tanh.

`weights`: Parameters of the model learned during training.

`inputs`: The features of the input data.

`bias`: An additional parameter in the model to adjust the output.

Convolutional Neural Networks (Cnn)

In the domain of IoT malware detection, CNN requires that the dataset be transformed into a form akin to an image or time-series data to facilitate convolution operations (Ghorsad & Zade, 2023). This necessitates preprocessing steps, such as scaling the data and organizing it into a grid-like structure, suitable for CNNs. These networks excel in extracting both spatial and temporal features, which are essential for identifying distinct malware patterns. The design of the CNN architecture includes setting up convolutional layers, each defined by specific hyperparameters such as the size of the filters and the stride length. The training phase of the CNN involves careful adjustment of various parameters, including the learning rate and the size of the data batches processed at a time.

The effectiveness of CNNs in IoT malware detection lies in their ability to process large volumes of data efficiently. This is particularly important in the IoT context, where devices generate vast amounts of data continuously. Likewise, the deployment of these models in real-world scenarios requires careful consideration of computational constraints, especially in resource-limited IoT devices. Thus, optimizing the CNN models for faster processing without compromising accuracy becomes a key aspect of IoT malware detection. Moreover, ongoing

research and advancements in CNN techniques are further enhancing their capability to detect even the most sophisticated malware in IoT environments.

$$ConvLayer_{output} = f(weights * input + bias)$$ [eq. 2]

In a CNN, the output of a convolutional layer, denoted as `$ConvLayer_{output}$`, emerges from processing the input, which could be an input image or a feature map. This processing involves the application of filters or kernels, referred to as `$weights$`, to the input. Following this convolution, an activation function, symbolized by `$f$`, is applied to introduce non-linearity to the system. Also, a bias term, simply termed as `bias`, is added to the output of the convolution to adjust the output signal.

Recurrent Neural Networks (Rnn) and Variants (Lstm, Bi-Lstm, Gru)

RNNs and their derivatives are highly effective for handling sequential data in IoT networks, necessitating the preprocessing of time-series data (Ghorsad & Zade, 2023), Ahn & Park, 2021). The feature engineering process in this context emphasizes capturing temporal dependencies within the data. Long Short-Term Memory networks (LSTMs) address the vanishing gradient challenge found in traditional RNNs, making them particularly suitable for processing extended sequences. Bidirectional LSTMs (Bi-LSTMs) take this further by analyzing data in both forward and reverse directions, offering a more comprehensive under-standing of the sequence. Gated Recurrent Units (GRUs) present a more streamlined option compared to LSTMs, with a reduced number of parameters yet maintaining efficiency. Training these networks involves careful selection of various parameters, including the number of hidden units and the learning rate.

The adaptability of RNNs and their variants to IoT applications is crucial due to the dynamic and continuous nature of data generated in IoT environments. Their ability to remember and utilize historical information makes them ideal for predicting future events or detecting anomalies in IoT networks. Besides, as IoT devices and net-works grow in complexity, these neural networks must be optimized to balance computational efficiency with predictive accuracy. This involves not only fine-tuning model parameters but also innovating model architecture to handle the increasing scale and complexity of IoT data.

$$LSTM_{output} = f(input, previousoutput, previousstate)$$ [eq. 3]

The term `$LSTM_{output}$` refers to the output generated by the unit. The LSTM processes data using an internal function, represented as `$f$`, which incorporates various gates for managing the flow of information. The `input` in this scenario is the current data being fed into the unit. Also, the LSTM unit considers `$previous\ output$`, which is the output from the immediately preceding time step, as well as the `$previous\ state$`, denoting the hidden state carried over from the previous time step. This combination of inputs and states allows the LSTM to effectively remember and integrate past information with current data.

Attention Mechanisms and Transformer Networks

Transformers, known for their attention-based mechanisms, excel in managing extensive IoT cybersecurity datasets, thanks to their ability to process data in parallel (Wang et al., 2022). The initial steps in data handling involve tokenizing the input and applying positional encodings. In feature engineering, the self-attention mechanism of Transformers is key, effectively addressing long-distance dependencies in the data. These models are structured with various attention

heads and multiple layers. The training phase concentrates on fine-tuning aspects such as the count of attention heads and the depth of the layers. The scalability of Transformers makes them particularly suitable for the ever-growing volumes of data in IoT networks. Their architecture allows for the efficient handling of both real-time and historical data, which is crucial for diverse IoT applications. Further, advancements in Transformer models pave the way for more sophisticated analyses in IoT systems. This includes enhanced real-time decision-making capabilities and improved predictive analytics. In optimizing these models, a balance must be struck between computational demands and the precision of insights derived, especially considering the resource constraints often present in IoT environments. This encompasses not only adjusting model parameters but also innovating in terms of reducing computational overhead while maintaining or enhancing model performance.

$$\text{Attention}(Q, K, V) = \text{softmax}\left(\frac{QK^T}{\sqrt{d_k}}\right)V \quad \text{[eq. 4]}$$

Here,
Attention`: The attention mechanism output.
Q`: Query matrix.
K`: Key matrix.
V`: Value matrix.
d_k`: Dimension of the key vectors, used for scaling.
softmax`: Normalization function.

Siamese Networks

In IoT anomaly detection, Siamese networks function (Kotiyal et al., 2023) by processing pairs of input data, designed to underscore similarities or disparities. Feature engineering in this context is directed at extracting distinctive features from these paired inputs. The architecture comprises two mirror subnetworks that share weights. The training phase is centered around contrastive loss, fine-tuning the network to effectively distinguish between pairs that are alike or different.

Siamese networks' ability to compare and contrast input pairs makes them particularly effective in identifying anomalies in IoT environments, where data consistency is key. Their shared-weight architecture not only aids in recognizing deviations from normal patterns but also ensures computational efficiency. This efficiency is vital in IoT settings, where resources might be limited. Besides, advancements in this field are continually refining these networks, enhancing their precision in detecting subtle anomalies. Optimizing these networks involves not just tweaking the contrastive loss function but also experimenting with different architectures and training methodologies to adapt to the diverse and progressing nature of IoT data. This ongoing evolution in Siamese network capabilities is crucial in maintaining robust security and operational integrity in IoT systems.

$$L(Y, Y', G) = Y \cdot \text{distance}(G) + (1 - Y) \cdot \max\big(0, m - \text{distance}(G)\big) \quad \text{[eq. 5]}$$

In the described context, the term `$L$` represents the contrastive loss function, which is a key component in determining the similarity between pairs in the model. The binary label `$Y$` indicates whether a pair is similar `$1$` or dissimilar `$0$`. In conjunction with this, `$Y'$` stands for the predicted similarity score, which is the model's estimation of how similar the pair is. The feature representation of the input pair is denoted as `$G$`, which is critical in understanding the characteristics of each pair. The function labeled as `distance` is used to measure the disparity between pairs within the embedding space. Finally, `$m$` refers to the margin parameter in the

contrastive loss function, which helps in defining the threshold for distinguishing between similar and dissimilar pairs.

Unsupervised Learning Models

Generative Adversarial Networks (Gan)

GNNs are primarily employed for generating synthetic network data in IoT set-tings. The initial stage includes normalizing real network data (Balaji & Narayanan, 2022). Since GNNs are inherently skilled at data generation, the requirement for extensive feature engineering is minimal. The principal architecture of GNNs is divided into two components: a generator and a discriminator. Their training follows a min-max approach, setting up a competitive scenario between these components, with crucial hyperparameters like the learning rate and the number of training epochs finely calibrated.

GNNs play a pivotal role in IoT cybersecurity, aiding in the development of solid security frameworks. By crafting realistic network traffic simulations, these networks contribute to generating more effective datasets for training, which consequently im-proves anomaly detection models. This capability is especially relevant in IoT contexts where data characteristics and volumes can significantly vary. Ongoing advancements in GNN technology, through refined training methods and architectural developments, are boosting their potential to accurately replicate complex and diverse net-work behaviors. This progress is essential in keeping pace with the ever-evolving cybersecurity challenges in the IoT sphere. Also, optimizing these models for IoT use not only involves enhancing their data generation proficiency but also ensuring computational efficiency, a critical factor given the resource constraints often present in IoT devices.

$$\min_G \max_D V(D,G) = E_{x\sim p_{data}(x)}[\log D(x)] + E_{z\sim p_z(z)}\left[\log\left(1 - D\left(G(z)\right)\right)\right] \quad \text{[eq. 6]}$$

Equation 6 represents that there are two primary components: `G`, the generator network, and `D`, the discriminator network. These two networks engage in a sort of game, quantified by the value function `V`, which represents the interaction between the generator and the discriminator. In this setup, `x` refers to real data samples that the discriminator evaluates. The generator, on the other hand, takes in a latent space vector `z` as input. This process involves two probability distributions: `$p_{data}$`, which is the probability distribution of the real data, and `$p_z$`, the probability distribution of the generator's input. These elements work together, with the generator trying to produce data similar to the real samples, and the discriminator attempting to distinguish between real and generated data.

Autoencoders and Variants (Sae, Dae, Cae, Vae)

Autoencoders (AEs) play a critical role in feature extraction and reducing data dimensions. The process begins with normalizing data, with Denoising Autoencoders (DAEs) additionally incorporating noise. Various AE types are tailored for specific ap-plications: Stacked Autoencoders (SAEs) feature multiple encoding layers, Convolutional Autoencoders (CAEs) are designed for processing convolutional data, and Variational Autoencoders (VAEs) implement a probabilistic dimension. Their architecture generally consists of an encoder and a decoder, and training is aimed at reducing re-construction loss while optimizing parameters such as learning rate and layer sizes (Haseeb et al., 2022). The ability of AEs to efficiently extract essential features and compress data is vital in handling the extensive and intricate datasets typical in IoT settings. Different AE models

tackle unique data processing issues, like DAEs improving resistance to noise, a common challenge in IoT. Ongoing enhancements in AE techniques, including architectural upgrades and training process improvements, are essential. These developments bolster the proficiency of AEs in managing a range of complex IoT applications, ensuring that these systems stay effective and efficient in the fast-evolving landscape of IoT data.

$$\text{Reconstruction Loss} = \left|\left|x - \hat{x}\right|\right|^2 \quad \text{[eq.7]}$$

Here,

`Reconstruction Loss`: Measure of how well the AE reconstructs the input.

`x`: Original input data.

`$\hat{x}$`: Reconstructed data from the AE.

Self-Organizing Maps (Som)

SOMs are essential for grouping and depicting complex, high-dimensional data. The initial stages of handling this data often involve normalization and sometimes the selection of particular features. Through unsupervised learning, SOMs self-organize, shedding light on the data's intrinsic structure. Adjusting the network's scale and the learning rate is a key focus during their training. SOMs excel at uncovering patterns and correlations in intricate IoT cybersecurity datasets, which can be difficult to detect (X. Qu et al. 2019). They efficiently transform high-dimensional data into a more manageable, low-er-dimensional format, aiding in the simplification and interpretation of large data volumes. The continual evolution of SOM techniques is enhancing their use in IoT contexts, particularly as they are combined with other machine learning methods for deeper data analysis. The ongoing refinement of their training processes and structural parameters is critical, ensuring that SOMs stay effective and relevant in the dynamic field of IoT. This evolution includes optimizing them for prompt data processing and adapting them to various kinds of IoT data sources.

$$\text{SOM}_u = \sum\left(x_i - w_{u,i}\right)^2 \quad \text{[eq. 8]}$$

Here,

`$SOM_u$`: Mapping function of SOM for neuron `u`.

`$x_i$`: Input vector.

`$w_{u,i}$`: Weight vector of neuron `u`.

Restricted Boltzmann Machine (Rbm) and Deep Belief Networks (Dbn)

RBMs and DBNs, which include variants like AE-DBN and RBM-DBM, excel in feature extraction and representation learning from unstructured data (Balakrishnan et al., 2021). The preprocessing for these models usually involves data normalization and binarization. RBMs utilize a hidden layer to understand the probability distribution of input data. In contrast, DBNs are formed by layering multiple RBMs or autoencoders. RBMs are trained using contrastive divergence, whereas DBNs benefit from a layer-by-layer training approach. Expanding on their utility, RBMs and DBNs are exceptionally adept at unraveling the intricate and often nonlinear patterns found in unstructured IoT data. Their capacity to restructure this data into a more coherent and analyzable form is key for further analysis and decision-making in IoT frameworks.

$$p(h|v) = \text{sigmoid}(\text{weights} \cdot v + \text{bias}) \quad \text{[eq. 9]}$$

The term $p(h|v)$ represents the probability of the hidden layer's state given the state of the visible layer in a neural network model. The activation function used here is the sigmoid

function, which helps in transforming the input signals into a format that is more manageable for the network. The weights are the model parameters that play a critical role in determining the strength and direction of the signal between neurons. The visible layer neurons, denoted as v, are the initial point of data entry into the model. Later, a bias term is included, which serves to adjust the output of the neuron, adding an additional degree of freedom to the model's fitting process.

Cluster-Based Networks

In the framework of IoT, networks tailored for unsupervised classification demand extensively preprocessed data, typically normalized. These networks employ clustering algorithms as part of their structure to aid in feature learning. The training phase encompasses a dual approach, focusing on optimizing both the network's weights and the assignments of clusters Castiglione, & Palmieri, 2021).

Delving deeper, such networks excel in detecting natural groupings and patterns within IoT data, bypassing the need for pre-assigned labels. They utilize advanced algorithms adept at pinpointing subtle nuances in the data, grouping them into relevant clusters. Normalizing the data is essential for these networks to uniformly handle data of varying scales. Training involves a careful calibration of both honing the cluster configurations and tweaking the network's internal parameters to ensure precise and effective categorization. This method is particularly pertinent in IoT settings, characterized by large, diverse datasets often devoid of clear labels.

$$\text{Cluster Loss} = \sum\left(x_i - c_{k_i}\right)^2 \qquad \text{[eq. 10]}$$

At this point,

(x_i): Represents an individual data point in the dataset. In the context of IoT cybersecurity, this is a feature vector extracted from network data.

(c_{k_i}): Denotes the center of the cluster to which the data point (x_i) is assigned. This is the 'representative' of the cluster, typically computed as the mean of all points assigned to that cluster.

$(\sum)$: Indicates a summation over all data points in the dataset. This ensures that the loss accounts for the distances of all points from their respective cluster centers.

$\left(x_i - c_{k_i}\right)^2$: This term computes the squared Euclidean distance between a data point and its cluster center. Squaring the distance emphasizes larger discrepancies, making the algorithm sensitive to outliers and ensuring tighter clusters.

Hybrid Learning Models

Model-A (Cnn + Lstm)

This hybrid model combines the spatial feature extraction capabilities of CNNs with the temporal learning of LSTMs, ideal for IoT data with both spatial and temporal dimensions. Preprocessing includes segmenting data into suitable formats for both CNN and LSTM layers. Feature engineering leverages CNN for initial extraction, followed by LSTM for sequential learning. Training involves optimizing both CNN and LSTM parameters, focusing on loss functions that cater to both spatial and temporal accuracies.

$$\text{Hybrid Output} = \text{LSTM}\big(\text{CNN}(input)\big) \qquad \text{[eq. 11]}$$

In this scenario, the term `Hybrid Output` refers to the final result produced by a model that integrates a CNN and a LSTM network. Initially, the `input` data, which is appropriate for CNN processing, is handled by the CNN. This Convolutional Neural Network is responsible for processing the initial input through its layers. Following this, the output from the CNN is then fed into the LSTM network. The LSTM, known for its ability to handle sequential data and remember long-term dependencies, processes the information received from the CNN. The culmination of this process is the `Hybrid Output`, which combines the strengths of both the CNN and LSTM networks to provide a comprehensive analysis of the input data.

Model-B (GAN + CNN)

Combining GANs with CNNs, this model is used for generating and classifying IoT data. GANs generate synthetic samples for training, while CNNs classify. Preprocessing involves training GANs on real data to produce realistic synthetic samples. CNNs are then trained on both real and synthetic data, with feature extraction focused on the convolutional layers. Training involves first optimizing GANs for realistic data generation, followed by CNN training for accurate classification.

$$\text{Classification Output} = \text{CNN}\big(\text{GAN}(input)\big) \quad \text{[eq. 12]}$$

`$Classification\ Output$` is the final output, typically a class label, from the CNN, that is used for classification. Whereas the GNN is used to generate synthetic data. In such scenarios, the $Input$ to the GAN, usually is a noise vector or latent representation.

Model-C (AE + SVM)

This model combines autoencoders for feature reduction and SVMs for classification. Preprocessing involves normalizing IoT data, with autoencoders trained to reduce dimensionality. SVMs then classify data in this reduced space. Feature engineering is focused on the latent space of the autoencoder. Training involves two stages: optimizing the autoencoder for accurate feature representation and then training the SVM on this reduced feature set.

$$\text{SVM Classification} = \text{SVM}\big(\text{AE}(input)\big) \quad \text{[eq. 13]}$$

`$SVM\ Classification$` is the classification result from the Support Vector Machine that is used for classification. Whereas autoencoder is employed for dimensionality reduction

Deep Transfer Learning (Dtl)

DTL involves applying knowledge gained from one area to a different but related problem, especially useful in IoT where labeled data can be scarce. Preprocessing involves adapting data from the source and target domains. Feature engineering focuses on extracting features that are relevant to both domains. Training involves fine-tuning pre-trained models on the target IoT dataset, optimizing for generalization between source and target domains (Yang at al., 2022).

$$\text{Target Output} = \text{DTL Model}(input) \quad \text{[eq. 14]}$$

Here,

Target Output`: The output for the target task in transfer learning.

DTL Model`: The deep learning model adapted from a source task to a target task.

input`: Input data for the target task.

Deep Reinforcement Learning (Drl) (Model-Based And Model-Free)

DRL is utilized for making decisions in IoT settings. In model-based DRL, there is a focus on acquiring knowledge about the environment's model, whereas model-free DRL concentrates on directly mastering the optimal policy. The preprocessing step encompasses the encoding state and action spaces. The training process is centered around refining a policy function in relation to a logic function, typically involving a process of trial and error, where the policy is modified according to the rewards received.

$$Q(s,a) = Q(s,a) + \alpha\left[r + \gamma \max_{a'} Q\,(s',a') - Q(s,a)\right] \quad \text{[eq. 15]}$$

In this framework, `$Q(s,a)$` represents the Q-value, which is a measure of the expected utility of acting `$a$` in state `s` within a reinforcement learning basis. The learning rate, denoted by `$\alpha$`, determines the extent to which new information overrides old information. After taking action `$a$` in state `$s$`, the agent receives a logic, symbolized by `$r$`. The discount factor, `$\gamma$`, is used to diminish the value of future rewards, reflecting the preference for immediate logic over distant ones. Following the action `a`, the agent transitions to a new state, referred to as `$s'$`. In this new state, `$a'$` represents the set of possible actions that the agent can take. This framework helps in evaluating and updating the policy the agent follows to maximize logic over time.

Federated Learning Models

In distributed IoT settings where data privacy is paramount, these models excel. Here, data stays on the individual devices, and only updates to the model are exchanged. The preprocessing step involves normalizing data locally. Both feature engineering and training occur on each device independently. The global model is refined by combining these local updates, aiming for a model that effectively works with the varied data from all involved devices (Wei, Xie, & Diao, 2023).

$$\text{Global Model} = \text{Aggregate}(\text{Local Models}) \quad \text{[eq. 16]}$$

Here,

`Global Model`: The aggregated model after federated learning.

`Aggregate`: Function to combine local model updates.

`Local Models`: Models trained on local devices with local data.

Each of these models presents unique attributes and challenges, necessitating specific considerations in data handling, feature engineering, and training, making them suitable for different aspects of IoT cybersecurity.

Data Collection and Preprocessing

Data Collection

For a deep learning-based cybersecurity system in IoT, selecting the right data collection methods is crucial. Data is primarily sourced from network traffic, the behavior of IoT devices, and interactions of users within the IoT network. Key activities include monitoring data packets, system logs, and sensor data in real time. The focus in data collection is on ensuring diversity, high volume, and rapid acquisition of data to enable thorough anomaly detection.

Identifying irregularities, like atypical network traffic or abnormal device operations, is essential for training deep learning algorithms to spot potential security risks. The goal of data collection is to encompass a broad spectrum of both standard and malicious actions, thereby providing a rich dataset for the deep learning system to effectively identify and adapt to new cybersecurity challenges. This method establishes a strong, forward-looking defense against complex cyber threats in IoT settings.

$$Data_{IoT} = (x_i, y_i) | x_i \in IoTtrafficormalwaresamples, y_i \in benign, malicious \quad \text{[eq. 17]}$$

Equation 17 represents the creation of a dataset, where each element is a pair $(\mathrm{x_i}, \mathrm{y_i})$. Here, $\mathrm{x_i}$ stands for individual samples of IoT network traffic or malware, and $\mathrm{y_i}$ is the label indicating whether each sample is benign or malicious.

Data Processing

Data processing involves several key steps. Initially, data normalization standardizes diverse datasets, ensuring uniformity for analysis. Feature extraction then isolates relevant attributes from this data, crucial for effective learning. Anomaly detection algorithms are applied to identify deviations from normal behavior, flagging potential security threats. This process often utilizes techniques like clustering, classification, or neural networks. The processed data then feeds into deep learning models for training, enhancing their ability to detect and predict complex cyber threats. Post-processing includes aggregation and interpretation of model outputs to refine threat identification. Throughout this pipeline, scalability, real-time processing capabilities, and handling high-dimensional data are vital considerations to maintain system efficacy and adaptability in dynamic IoT environments.

$$Data_{processed} = f_{preprocess}(Data_{IoT}) \quad \text{[eq. 18[}$$

This shows the transformation of the collected data into a set-up appropriate for the deep learning model. The function $\mathrm{f}_{preprocess}$ includes operations like cleaning, normalization, and other transformations.

Deep Learning Model Progression for Iot Security

To formalize the progression of a deep learning model for IoT network security, we have devised mathematical representations for each of the steps involved. These simplified equations provide a concise and rigorous framework for understanding and implementing the model development process:

Feature Engineering

Feature Extraction

A range of anomalous features can be extracted to feed into DL systems for an effective IDS. These features include unusual data packet sizes, irregular transmission frequencies, deviations in power consumption patterns, unexpected device reboots or shutdowns, anomalies in sensor readings that deviate from established patterns, irregularities in API call sequences, unexpected changes in network topology, unusual pat-terns in user access and authentication activities, spikes or drops in data flow rates, and inconsistencies in firmware update patterns. Likewise, unusual behavior in inter-device communication, discrepancies in geographical location data, and atypical usage of system resources can also serve as indicators of potential security breaches or malicious activities in the IoT network.

$$F = extract_{features}\left(Data_{processed}\right) \quad \text{[eq. 19]}$$

Eq. 19 represents the abstraction of applicable features from the processed data. These features are critical for distinguishing between benign and malicious samples.

Dimensionality Reduction (E.G., Pca)

Principal Component Analysis (PCA) is applicable to identify key features in a dataset, known as principal components. These components are new, uncorrelated variables created as linear combinations of the original features, and they're arranged in a way that the initial few account for most of the variation found in the entire set of original variables. PCA's approach of selecting only the primary components significantly reduces the complexity of the feature space while retaining crucial data attributes. This streamlined data is easier to analyze and use for model training, addressing challenges like overfitting and high computational needs. PCA excels in distilling essential elements from intricate datasets, enhancing deep learning models' efficiency in cybersecurity scenarios, as shown in eq. 20.

$$F_{reduced} = PCA(F) \quad \text{[eq. 20]}$$

In IoT systems employing deep learning for IDS, the feature set's dimensionality can be extensive due to a variety of features, like abnormal packet sizes or sensor reading anomalies. This high dimensionality complicates model training, increases computational load, and heightens the risk of overfitting. Dimensionality reduction is thus crucial, using methods like PCA, wrapper, filter, and embedded techniques for feature selection. By decreasing dimensionality, these methods streamline the learning process, improve the model's generalization capabilities from training data, and expedite processing. This makes the IDS more effective for real-time threat detection in IoT contexts.

Model Selection and Architecture Design

Model Selection

$$\text{Model} = \text{choose}_{\text{model}}(\text{CNN}, \text{RNN}, \text{LSTM}, \ldots) \quad \text{[eq. 21]}$$

Equation 21 represents the selection process for an appropriate deep learning model architecture, such as CNN, RNN, LSTM, etc., based on the nature of the data and the precise requirements of the task.

Architecture Design For A Cnn Example

$$\text{CNN} = \text{Sequential}([\text{ConvLayer}, \text{Activation}, \ldots, \text{DenseLayer}]) \quad \text{[eq. 22]}$$

For a CNN model , this outlines the sequential arrangement of various layers, including convolutional layers, activation functions, and fully connected (dense) layers.

Model Training and Hyperparameter Optimization

Data Splitting

$$\text{Data}_{\text{train}}, \text{Data}_{\text{val}}, \text{Data}_{\text{test}} = \text{split}\left(\text{Data}_{\text{processed}}\right) \quad \text{[eq. 23]}$$

Equation 23 illustrates the division of the processed data into training, validation, and testing sets, a critical step in training and evaluating the model.

Model Training

$$Model_{trained} = train(Model, Data_{train}, Hyperparameters) \quad \text{[eq. 24]}$$

This represents the training of the model using the training dataset and a set of hyperparameters.

Performance Evaluation

$$Performance = evaluate(Model_{trained}, Data_{val}) \quad \text{[eq. 25]}$$

This equation illustrates the evaluation of the trained model's performance using the validation dataset, which is crucial for preventing overfitting and tuning the model's hyperparameters.

Hyperparameter Optimization

Hyperparameter Optimization (E.G., Grid Search)

$$\mathbf{Hyperparameters_{optimal}} = \text{argmax}_{\text{Hyperparametersevaluate}}(\text{Model}, \text{Data}_{\text{val}}, \text{Hyperparameters}) \quad \text{[eq. 26]}$$

The equations [1-26] reflect a high-level abstraction of the deep learning model development process, focusing on the essential components of data processing, feature engineering, model design, and optimization in the context of IoT security. The progression of a deep learning model for IoT network security involves several crucial steps. It begins with data collection and preprocessing, where a dataset comprising both benign and malicious IoT network traffic or malware samples is gathered. This dataset is then cleaned, normalized, and transformed to be suitable for deep learning analysis. Next is feature engineering, where key features that can distinguish between benign and malicious entities are extracted, and techniques like dimensionality diminution are applied to manage the intricacy of the data. The third step involves selecting an appropriate deep learning model, such as CNNs or RNNs, and designing its architecture, including layer types and activation functions. Ultimately, the model is trained using the processed data, with a focus on optimizing hyperparameters to enhance its performance. This training involves splitting the data into subsets for training, validation, and testing, ensuring the model is robust and accurate in identifying security threats in IoT networks.

Machine Learning Vs. Deep Learning In Iot Security

In comparing machine learning (ML) and deep learning (DL) in the context of IoT security, it's crucial to recognize their distinct roles and capabilities (Thakkar & Lohiya, 2020), (Sharmaet al., 2021), (Sarker et al., 2022), (Alex et al., 2023). ML, encompassing both supervised and unsupervised approaches, has been instrumental in addressing various security challenges in IoT. Supervised methods like Decision Trees (DTs), Support Vector Machines (SVMs), Naive Bayes (NB), K-Nearest Neighbors (KNN), Random Forests (RF), and Ensemble Learning (EL) are adept at classifying and predicting based on labeled data. Unsupervised techniques, such as k-means clustering and Principal Component Analysis (PCA), excel in anomaly detection and pattern discovery without prior labeling.

Deep learning, an advanced subset of ML, extends these capabilities through its hierarchical learning approach. In supervised contexts, deep learning employs ANNs, CNNs, and RNNs to analyze complex and high-dimensional data. Unsupervised deep learning methods like AEs, RBMs, and DNMs are highly effective in feature extraction and data representation. Hybrid

approaches, including GANs and Ensemble Deep Learning Networks (EDLNs), leverage the strengths of both supervised and unsupervised learning for enhanced performance.

Table 6 offers a comprehensive comparison of ML and DL models within the scope of IoT security, addressing various attack surfaces: the Perception, Network, and Application Layers. The Perception Layer, also known as the physical layer, involves data collection via sensors and actuaries. It faces threats like false data injection and device identity spoofing. To combat these, strategies like data validation, robust authentication protocols such as IEEE 802.15.4, and cryptographic algorithms are utilized to ensure data integrity and mitigate tampering risks.

At the Network Layer, which facilitates data transmission between devices and the cloud, vulnerabilities include routing, jamming, and DDoS attacks. Enhancing security here involves fortifying IoT communication protocols like MQTT and CoAP with TLS/SSL encryption and secure routing protocols. Machine learning models play a pivotal role in detecting anomalies in network traffic, indicative of potential cyberattacks.

The Application Layer, the interface for data processing and user interaction, is susceptible to malware and intrusion attempts. Protocols like OAuth and HTTPS are crucial for maintaining secure communication and authorization. In this context, DL models like CNNs and RNNs are increasingly employed for their advanced intrusion detection capabilities and for analyzing anomalous behaviors, adapting to new threats.

Table 6 Comparative Analysis of Machine and Deep Learning Models for IoT Security Across Various Attack Surfaces.

Threats/Security Application	ML: Supervised Approaches	ML: Unsupervised Approaches	DL: Supervised Approaches	DL: Unsupervised Approaches	DL: Hybrid Approaches
Routing Attack Detection	✓	✓	✓	✓	✓
Signal Disruption Attacks	✓	X	✓	✓	✓
Incorrect Information Insertion	✓	X	✓	✓	✓
Penetration Discovery	✓	✓	✓	✓	✓
Malicious Conduct Identification	✓	✓	✓	✓	✓
Information Manipulation	✓	✓	✓	✓	✓
Deception Attack Identification	✓	X	✓	✓	✓
Malicious Software Discovery	✓	X	✓	✓	✓
Impersonation Attacks	✓	X	✓	✓	✓
Cyberattacks	✓	✓	✓	✓	✓
Network Irregularity Identification	✓	✓	✓	✓	✓
DDoS Attack Identification	✓	✓	✓	✓	✓
Verification	✓	X	✓	✓	✓
IoT Device Recognition	✓	X	✓	✓	✓

The Table 6 underscores the efficacy of both ML and DL models in addressing IoT security challenges. Super-vised ML methods are versatile but often rely on extensive labeled data.

Unsupervised ML is adept at uncovering hidden patterns, though its effectiveness may vary with specific threat types. DL models, in both supervised and unsupervised forms, excel in processing complex, large-scale data. Hybrid DL methods offer a synergistic approach, blending the strengths of both supervised and unsupervised learning for robust security solutions in even the most challenging scenarios. This detailed analysis serves as a vital resource for computer science researchers in picking the seemliest models for specific security challenges in the IoT landscape.

Datasets and Tools for Iot Security

Selecting the right datasets is a critical factor in the efficacy of deep learning models in IoT security. A variety of datasets, including NSL-KDD, UNSW-NB15, BotnetIoT-01, BotIoT, TON-IoT, Edge-IIoT, UNSW2015, IoT-23, MQTTSet, MQTT-IoT-IDS2020, Large-scale Urban IoT Activity Data, and IoT Traffic Dataset for Zigbee Protocol, provide a range of features and challenges for these models (Wang et al., 2022), (De Keersmaeker et al., 2023), (Bellman & van Oorschot, 2023). These datasets vary in their feature selection techniques; while NSL-KDD and UNSW-NB15 offer extensive features necessitating complex selection methods, IoT-23 and MQTTSet focus on IoT-specific features, offering simplicity but less diversity.

Datasets such as TON-IoT and Edge-IIoT, which include Netflow features, are invaluable for anomaly detection in IoT networks, but processing these features can be resource-intensive. Addressing class imbalances in datasets like BotnetIoT-01 and BotIoT is crucial, often requiring techniques like oversampling or synthetic data generation, which, while effective, can introduce bias. The size and diversity of a dataset, such as UNSW2015 and Large-scale Urban IoT Activity Data, are fundamental for model generalization, though they come with higher computational demands.

The computational load is a concern, especially with large and complex datasets like the IoT Traffic Dataset for Zigbee Protocol. Detection rates and accuracy also differ among datasets; for instance, MQTT-IoT-IDS2020 is known for high accuracy but might not fully capture the complexity of real-world scenarios. Certain datasets are designed for specific IoT scenarios, like Edge-IIoTSet for edge computing, limiting their broader applicability.

A key limitation in current datasets is their inability to fully represent the dynamic nature of real-world IoT environments and the evolving spectrum of cyber threats. Therefore, the ideal dataset to combat IoT cybersecurity threats should blend a variety of real-world data, IoT-specific features, and diverse attack scenarios. It should comprehensively cover different IoT devices and protocols and include both time-series and network flow data for a complete analysis.

Looking forward, the development of IoT cybersecurity datasets should lean towards integrating real-time data, encompassing a wider array of IoT protocols and devices, and keeping pace with changing threat landscapes. Emphasizing datasets that replicate the dynamics of actual IoT networks, including edge computing scenarios, will be vital. Encouraging the formation and growth of open-source communities for sharing and collaboratively enhancing datasets will be instrumental in advancing the development and validation of deep learning models in IoT security.

Future of Iot Security with Deep Learning

Based on earlier discussions, we foresee following DL enabled IoT cybersecurity paradigm:

a) DL models can be trained on diverse data types, including text, images, and sensor readings, to provide a more comprehensive view of IoT network activity.

b) Active learning techniques are/can be employed to optimize the data collection process for DL models, minimizing the amount of data required for training while maintaining model performance. This approach reduces storage and computational overhead, particularly in resource-constrained IoT environments.
c) Emerging trends and advanced technologies are set to significantly enhance the landscape of IoT security, particularly through the integration of deep learning. Federated Learning (FL) emerges as a key innovation, facilitating a decentralized approach to training deep learning models across multiple IoT devices. This method maintains data privacy by keeping the training data localized, thus improving the security architecture without compromising data privacy. In FL framework, Differential Privacy plays a vital role by mathematically ensuring the protection of individual data points during analysis, adding a layer of security by preventing sensitive information disclosure in deep learning outputs.
d) Explainable AI (XAI) is revolutionizing deep learning in IoT security by ad-dressing the challenge of model transparency. With XAI, the decision-making processes of AI models become interpretable and accountable, crucial for gaining trust and adhering to regulatory standards. This transparency is especially important for IoT security, as it allows for the identification of biases and ensures fairness in automated decisions.
e) Blockchain technology contributes significantly to this security paradigm by providing a secure, transparent, and tamper-proof system for recording transactions and managing IoT device identities. Its integration with IoT and deep learning creates a robust framework for verifying and tracing data ex-changes, greatly reducing unauthorized access and tampering risks.
f) Complementing these is Edge Computing, which optimizes data processing by performing it closer to the data source. This reduces latency and limits data exposure, enhancing the efficiency of real-time security analyses and decision-making in deep learning models. Edge computing, therefore, plays a critical role in enabling swift responses to security threats in IoT environments.
g) Privacy-preserving techniques can/will be integrated into DL algorithms to ensure the protection of sensitive data in IoT environments. These techniques enable secure processing and analysis of data without compromising privacy, addressing concerns about data breaches and unauthorized access.
h) GNNs are gaining attention in IoT cybersecurity due to their ability to effectively model and analyze the complex relationships and interactions between IoT devices in a network. GNNs can identify patterns and anomalies in net-work traffic and device interactions, enabling early detection of cyberattacks and potential security vulnerabilities.
i) DL-powered self-healing capabilities (i.e., autonomic behavior) can be incorporated into IoT networks to enable automated recovery from cyberattacks. These self-healing mechanisms can detect and isolate compromised devices, remediate vulnerabilities, and restore normal network functionality without requiring manual intervention.
j) DL can be applied to address security challenges in Cyber-Physical Systems (CPS), which integrate physical infrastructure with computational elements. DL-based anomaly detection and threat identification can protect critical infrastructure from cyberattacks that could disrupt essential services and cause significant damage.
k) Lightweight DL models can be developed specifically for resource-constrained IoT devices, enabling real-time threat detection and anomaly analysis without compromising device performance or energy consumption. These models are tailored to the limited processing power and memory constraints of IoT devices.
l) Hardware accelerators, such as Field Programmable Gate Arrays (FPGAs) and Application-Specific Integrated Circuits (ASICs), can be employed to accelerate DL computations in IoT devices, enabling real-time security processing and reducing latency.

m) Adversarial Machine Learning (AML) techniques can be used to enhance the robustness of DL-powered IoT security systems against evasive attacks. These techniques enable models to detect and defend against attacks that attempt to manipulate or obfuscate data to evade detection.

Consequently, the convergence of these advanced technologies with deep learning promises a transformative impact on IoT security. Federated Learning and Differential Privacy will strengthen data privacy, XAI will provide much-needed transparency, Blockchain will secure data transactions, and Edge Computing will enable faster, more efficient threat responses. Collectively, these technologies formulate a comprehensive and advanced approach to safeguarding IoT ecosystems against the dynamic array of cybersecurity challenges.

Challenges and Limitations

While the adoption of deep learning in IoT cybersecurity marks a significant advancement, it is not without its technical and ethical challenges, as well as certain limitations in the existing research. Most prominent of the technical issues are as follows:

a) Deep learning models, particularly advanced ones like CNNs and RNNs, re-quire substantial computational power and memory, challenging for re-source-limited IoT devices. This dependence on cloud or edge computing can introduce latency and new security risks during data transmission.
b) Effective training of deep learning models necessitates large volumes of high-quality, characterized data. In IoT cybersecurity, acquiring such data is problematic due to privacy concerns and the sensitive nature of security data. Also, the need for continual model updates to combat evolving cyber threats poses challenges in maintaining model effectiveness.
c) The application of deep learning in IoT can lead to potential privacy breaches, necessitating strict data anonymization and adherence to privacy regulations like GDPR and HIPAA. There's also the risk of biased outcomes from AI models if the training data is not representative of real-world scenarios.
d) Deep learning models in IoT cybersecurity are often "black-boxes" with non-transparent decision-making processes. This lack of explainability is problematic in security contexts where understanding model predictions is crucial.
e) Current research primarily addresses conventional cyberattack patterns, with limited attention to more sophisticated or emerging attack vectors. This focus might leave IoT systems vulnerable to new types of cyber threats.
f) There's a significant requirement for research that integrates deep learning theory, cybersecurity expertise, and IoT technology. Much of the existing re-search is conducted in isolation, potentially leading to solutions that aren't fully practical in real-world IoT environments. Collaborative research efforts are essential to develop holistic cybersecurity solutions for the IoT landscape.

Conclusion and Future Directions

In the domain of IoT cybersecurity, the integration of DL has catalyzed significant advancements, particularly in enhancing anomaly detection, IDS, and malware recognition. Deep learning architectures like CNNs and RNNs have demonstrated remarkable efficacy in

extracting intricate features from high-dimensional IoT data, crucial for identifying and neutralizing sophisticated cyber threats. Advanced DL models, including GNNs and Transformer Models, are emerging as potent tools for understanding complex IoT network interactions and predicting potential vulnerabilities. These models, leveraging attention mechanisms, excel in interpreting inter-device relation-ships, are vital for comprehensive IoT security frameworks.

Future research in DL for IoT cybersecurity is poised to focus on developing lightweight, efficient models suitable for deployment in resource-constrained IoT de-vices, ensuring real-time threat detection without compromising performance. The exploration of Federated Learning and Edge Computing paradigms is crucial for maintaining data privacy while facilitating decentralized model training and faster decision-making. Moreover, the integration of XAL will be pivotal in ensuring transparency and trust in DL-driven security solutions. Continuous advancements in adversarial learning are expected to bolster DL model resilience against sophisticated evasion techniques. Addressing the challenges of dynamic IoT environments and evolving cyber threats, future research will likely converge on optimizing DL models for greater scalability, efficiency, and adaptability, ensuring robust protection for increasingly complex IoT ecosystems.

Author Contributions: Conceptualization, U.T. and I.A.; methodology, U.T., I.A. and A.K.B.; software, U.T., I.A. and M.A.K.; validation, U.T., I.A. and A.K.B.; formal analysis, U.T., I.A., A.K.B. and M.A.K.; resources, U.T.; data curation, U.T. and M.A.K.; writing—original draft preparation, U.T. and I.A.; writing—review and editing, U.T., A.K.B. and M.A.K.; visualization, U.T. and A.K.B.; supervision, U.T.; project administration, U.T. and funding acquisition, U.T. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Prince Sattam bin Abdulaziz University, Saudi Arabia through project number 2023/RV/8.

Institutional Review Board Statement: The study was conducted according to the guidelines of the Declaration of Deanship of Scientific Research, Prince Sattam Bin Abdulaziz University, Saudi Arabia.

Informed Consent Statement: This research study involves the collection and analysis of data obtained from published sources. No personal or confidential information from individual participants was used or required for this review.

Data Availability Statement: The data analyzed in this review are derived entirely from publicly available sources. Detailed references to all original studies and data sources are provided within the manuscript.

Acknowledgments: This study was sponsored by Prince Sattam bin Abdulaziz University through project number 2023/RV/8.

Conflicts of Interest: The authors declare no conflicts of interest relevant to this study. All funding sources have been disclosed in the Acknowledgements section of this manuscript.

References

Ahanger, Tariq Ahamed, Usman Tariq, Atef Ibrahim, Imdad Ullah, and Yassine Bouteraa. "IoT-Inspired Framework of Intruder Detection for Smart Home Security Systems." *Electronics* 9, no. 9 (August 21, 2020): 1361. https://doi.org/10.3390/electronics9091361.

Ahn, Hyung Keun, and Neungsoo Park. "Deep RNN-Based Photovoltaic Power Short-Term Forecast Using Power IoT Sensors." *Energies* 14, no. 2 (January 15, 2021): 436. https://doi.org/10.3390/en14020436.

Ahmad, Shahnawaz, Iman Shakeel, Shabana Mehfuz, and Javed Ahmad. "Deep Learning Models for Cloud, Edge, Fog, and IoT Computing Paradigms: Survey, Recent Advances, and Future Directions." *Computer Science Review* 49 (August 2023): 100568. https://doi.org/10.1016/j.cosrev.2023.100568.

Ali, Saif Mohammed, Amer S. Elameer, and Mustafa Musa Jaber. "IoT Network Security Using Autoencoder Deep Neural Network and Channel Access Algorithm." *Journal of Intelligent Systems* 31, no. 1 (December 8, 2021): 95–103. https://doi.org/10.1515/jisys-2021-0173.

Alex, Christin, Giselle Creado, Wesam Almobaideen, Orieb Abu Alghanam, and Maha Saadeh. "A Comprehensive Survey for IoT Security Datasets Taxonomy, Classification and Machine Learning Mechanisms." *Computers & Security* 132 (September 2023): 103283. https://doi.org/10.1016/j.cose.2023.103283.

Amanullah, Mohamed Ahzam, Riyaz Ahamed Ariyaluran Habeeb, Fariza Hanum Nasaruddin, Abdullah Gani, Ejaz Ahmed, Abdul Salam Mohamed Nainar, Nazihah Md Akim, and Muhammad Imran. "Deep Learning and Big Data Technologies for IoT Security." *Computer Communications* 151 (February 2020): 495–517. https://doi.org/10.1016/j.comcom.2020.01.016.

Aversano, Lerina, Mario Luca Bernardi, Marta Cimitile, and Riccardo Pecori. "A Systematic Review on Deep Learning Approaches for IoT Security." *Computer Science Review* 40 (May 2021): 100389. https://doi.org/10.1016/j.cosrev.2021.100389.

Almaraz-Rivera, Josue Genaro, Jose Antonio Cantoral-Ceballos, and Juan Felipe Botero. "Enhancing IoT Network Security: Unveiling the Power of Self-Supervised Learning against DDoS Attacks." *Sensors* 23, no. 21 (October 25, 2023): 8701. https://doi.org/10.3390/s23218701.

Audibert, Julien, Pietro Michiardi, Frédéric Guyard, Sébastien Marti, and Maria A. Zuluaga. "Do Deep Neural Networks Contribute to Multivariate Time Series Anomaly Detection?" *Pattern Recognition* 132 (December 2022): 108945. https://doi.org/10.1016/j.patcog.2022.108945.

Balaji, S., and S. Sankara Narayanan. "Dynamic Distributed Generative Adversarial Network for Intrusion Detection System over Internet of Things." *Wireless Networks* 29, no. 5 (November 23, 2022): 1949–67. https://doi.org/10.1007/s11276-022-03182-8.

Balakrishnan, Nagaraj, Arunkumar Rajendran, Danilo Pelusi, and Vijayakumar Ponnusamy. "Deep Belief Network Enhanced Intrusion Detection System to Prevent Security Breach in the Internet of Things." *Internet of Things* 14 (June 2021): 100112. https://doi.org/10.1016/j.iot.2019.100112.

Bellman, Christopher, and Paul C. van Oorschot. "Systematic Analysis and Comparison of Security Advice as Datasets." *Computers & Security* 124 (January 2023): 102989. https://doi.org/10.1016/j.cose.2022.102989.

Catillo, Marta, Antonio Pecchia, and Umberto Villano. "CPS-GUARD: Intrusion Detection for Cyber-Physical Systems and IoT Devices Using Outlier-Aware Deep Autoencoders." *Computers & Security* 129 (June 2023): 103210. https://doi.org/10.1016/j.cose.2023.103210.

Choudhary, Sarika, and Nishtha Kesswani. "Analysis of KDD-Cup'99, NSL-KDD and UNSW-NB15 Datasets Using Deep Learning in IoT." *Procedia Computer Science* 167 (2020): 1561–73. https://doi.org/10.1016/j.procs.2020.03.367.

Cheng, Pengzhou, Kai Xu, Simin Li, and Mu Han. "TCAN-IDS: Intrusion Detection System for Internet of Vehicle Using Temporal Convolutional Attention Network." *Symmetry* 14, no. 2 (February 3, 2022): 310. https://doi.org/10.3390/sym14020310.

Chen, Dongliang, Pawel Wawrzynski, and Zhihan Lv. "Cyber Security in Smart Cities: A Review of Deep Learning-Based Applications and Case Studies." *Sustainable Cities and Society* 66 (March 2021): 102655. https://doi.org/10.1016/j.scs.2020.102655.

Chaabouni, Nadia, Mohamed Mosbah, Akka Zemmari, Cyrille Sauvignac, and Parvez Faruki. "Network Intrusion Detection for IoT Security Based on Learning Techniques." *IEEE Communications Surveys & Tutorials* 21, no. 3 (2019): 2671–2701. https://doi.org/10.1109/comst.2019.2896380.

D'Angelo, Gianni, Arcangelo Castiglione, and Francesco Palmieri. "A Cluster-Based Multidimensional Approach for Detecting Attacks on Connected Vehicles." *IEEE Internet of Things Journal* 8, no. 16 (August 15, 2021): 12518–27. https://doi.org/10.1109/jiot.2020.3032935.

Damadam, Shima, Mojtaba Zourbakhsh, Reza Javidan, and Azadeh Faroughi. "An Intelligent IoT Based Traffic Light Management System: Deep Reinforcement Learning." *Smart Cities* 5, no. 4 (September 27, 2022): 1293–1311. https://doi.org/10.3390/smartcities5040066.

De Keersmaeker, François, Yinan Cao, Gorby Kabasele Ndonda, and Ramin Sadre. "A Survey of Public IoT Datasets for Network Security Research." *IEEE Communications Surveys & Tutorials* 25, no. 3 (2023): 1808–40. https://doi.org/10.1109/comst.2023.3288942.

Demirkıran, Ferhat, Aykut Çayır, Uğur Ünal, and Hasan Dağ. "An Ensemble of Pre-Trained Transformer Models for Imbalanced Multiclass Malware Classification." *Computers & Security* 121 (October 2022): 102846. https://doi.org/10.1016/j.cose.2022.102846.

Firat Kilincer, Ilhan, Fatih Ertam, Abdulkadir Sengur, Ru-San Tan, and U. Rajendra Acharya. "Automated Detection of Cybersecurity Attacks in Healthcare Systems with Recursive Feature Elimination and Multilayer Perceptron Optimization." *Biocybernetics and Biomedical Engineering* 43, no. 1 (January 2023): 30–41. https://doi.org/10.1016/j.bbe.2022.11.005.

Felcia Bel H.J., and Sabeen S. "A Survey on IoT Security: Attacks, Challenges and Countermeasures." *Webology* 19, no. 1 (January 20, 2022): 3741–63. https://doi.org/10.14704/web/v19i1/web19246.

Gordon, Lucas. "Leveraging Dual-Generative Adversarial Networks for Adversarial Malware Detection via Ensemble Learning." *Inquiry@Queen's Undergraduate Research Conference Proceedings* 17, no. 2 (August 29, 2023). https://doi.org/10.24908/iqurcp16688.

Ghorsad, Thamraj Narendra, and Amol V. Zade. "Hybrid CNN+LSTM Deep Learning Model for Intrusions Detection Over IoT Environment." *International Journal on Recent and Innovation Trends in Computing and Communication* 11, no. 10s (October 7, 2023): 01–11. https://doi.org/10.17762/ijritcc.v11i10s.7588.

Haseeb, Junaid, Masood Mansoori, Yuichi Hirose, Harith Al-Sahaf, and Ian Welch. "Autoencoder-Based Feature Construction for IoT Attacks Clustering." *Future Generation Computer Systems* 127 (February 2022): 487–502. https://doi.org/10.1016/j.future.2021.09.025.

Hassebo, Ahmed, and Mohamed Tealab. "Global Models of Smart Cities and Potential IoT Applications: A Review." *IoT* 4, no. 3 (August 31, 2023): 366–411. https://doi.org/10.3390/iot4030017.

Han, Xu, and Shicai Gong. "LST-GCN: Long Short-Term Memory Embedded Graph Convolution Network for Traffic Flow Forecasting." *Electronics* 11, no. 14 (July 17, 2022): 2230. https://doi.org/10.3390/electronics11142230.

He, Wenji, Yifeng Liu, Haipeng Yao, Tianle Mai, Ni Zhang, and F. Richard Yu. "Distributed Variational Bayes-Based In-Network Security for the Internet of Things." *IEEE Internet of Things Journal* 8, no. 8 (April 15, 2021): 6293–6304. https://doi.org/10.1109/jiot.2020.3041656.

Iliyasu, Auwal Sani, and Huifang Deng. "Semi-Supervised Encrypted Traffic Classification With Deep Convolutional Generative Adversarial Networks." *IEEE Access* 8 (2020): 118–26. https://doi.org/10.1109/access.2019.2962106.

Ilango, Harun Surej, Maode Ma, and Rong Su. "A FeedForward–Convolutional Neural Network to Detect Low-Rate DoS in IoT." Engineering Applications of Artificial Intelligence 114 (September 2022): 105059. https://doi.org/10.1016/j.engappai.2022.105059.

Jahwar, Alan Fuad, and Subhi R. M. Zeebaree. "A State of the Art Survey of Machine Learning Algorithms for IoT Security." *Asian Journal of Research in Computer Science*, June 16, 2021, 12–34. https://doi.org/10.9734/ajrcos/2021/v9i430226.

Kamala, J., and G. M. Kadhar Nawaz. "Secure Communication Using Multi-Layer Perceptron Neural Network and the Adaptive-Network-Based Fuzzy Inference System in Wireless Network." *SN Computer Science* 4, no. 6 (September 26, 2023). https://doi.org/10.1007/s42979-023-02121-4.

Khan, Saad, and Akalanka B. Mailewa. "Discover Botnets in IoT Sensor Networks: A Lightweight Deep Learning Framework with Hybrid Self-Organizing Maps." *Microprocessors and Microsystems* 97 (March 2023): 104753. https://doi.org/10.1016/j.micpro.2022.104753.

Kholidy, Hisham A. "Correlation-based Sequence Alignment Models for Detecting Masquerades in Cloud Computing." IET Information Security 14, no. 1 (January 2020): 39–50. https://doi.org/10.1049/iet-ifs.2019.0409.

Kotiyal, Vaibhav, Anshita Gupta, Pallav Kumar Deb, Subhas Chandra Misra, Debanjan Das, and Venkanna Udutalapally. "Skipper: A Federated Siamese Network-Based Group Activity Segregator for IoMT Systems." *IEEE Transactions on Computational Social Systems* 10, no. 4 (August 2023): 1770–79. https://doi.org/10.1109/tcss.2023.3244188.

Meidan, Yair, Michael Bohadana, Yael Mathov, Yisroel Mirsky, Asaf Shabtai, Dominik Breitenbacher, and Yuval Elovici. "N-BaIoT—Network-Based Detection of IoT Botnet Attacks Using Deep Autoencoders." *IEEE Pervasive Computing* 17, no. 3 (July 2018): 12–22. https://doi.org/10.1109/mprv.2018.03367731.

Moro, Lorenzo, and Enrico Prati. "Anomaly Detection Speed-up by Quantum Restricted Boltzmann Machines." *Communications Physics* 6, no. 1 (September 23, 2023). https://doi.org/10.1038/s42005-023-01390-y.

Murugiah, Premkumar, Akila Muthuramalingam, and S. Anandamurugan. "A Design of Predictive Manufacturing System in IoT-assisted Industry 4.0 Using Heuristic-derived Deep Learning." *International Journal of Communication Systems* 36, no. 5 (January 8, 2023). https://doi.org/10.1002/dac.5432.

Naeem, Muhammad Ali, Yousaf Bin Zikria, Rashid Ali, Usman Tariq, Yahui Meng, and Ali Kashif Bashir. "Cache in Fog Computing Design, Concepts, Contributions, and Security Issues in Machine Learning Prospective." *Digital Communications and Networks* 9, no. 5 (October 2023): 1033–52. https://doi.org/10.1016/j.dcan.2022.08.004.

Qiao, Yanchen, Weizhe Zhang, Xiaojiang Du, and Mohsen Guizani. "Malware Classification Based on Multilayer Perception and Word2Vec for IoT Security." *ACM Transactions on Internet Technology* 22, no. 1 (September 14, 2021): 1–22. https://doi.org/10.1145/3436751.

Puteho, Collins Sankwasa, Attlee Gamundani, and Isaac Nhamu. "Applying the NIST Cybersecurity Framework in Developing a Digital Forensic Incident Response Roadmap for the Security Sector in Namibia." *SSRN Electronic Journal*, 2023. https://doi.org/10.2139/ssrn.4332936.

Qu, Xiaofei, Lin Yang, Kai Guo, Linru Ma, Meng Sun, Mingxing Ke, and Mu Li. "A Survey on the Development of Self-Organizing Maps for Unsupervised Intrusion Detection." *Mobile Networks and Applications* 26, no. 2 (October 2, 2019): 808–29. https://doi.org/10.1007/s11036-019-01353-0.

Riandhanu, Ichsan Octama. "Analisis Metode Open Web Application Security Project (OWASP) Menggunakan Penetration Testing Pada Keamanan Website Absensi." Jurnal Informasi Dan Teknologi, October 3, 2022. https://doi.org/10.37034/jidt.v4i3.236.

Sudhakar, K., and S. Senthilkumar. "Weibull Distributive Feature Scaling Multivariate Censored Extreme Learning Classification for Malicious IoT Network Traffic Detection." *IETE Journal of Research*, April 20, 2023, 1–15. https://doi.org/10.1080/03772063.2023.2192426.

Syed, Naeem Firdous, Mengmeng Ge, and Zubair Baig. "Fog-Cloud Based Intrusion Detection System Using Recurrent Neural Networks and Feature Selection for IoT Networks." *Computer Networks* 225 (April 2023): 109662. https://doi.org/10.1016/j.comnet.2023.109662.

Sarker, Iqbal H., Asif Irshad Khan, Yoosef B. Abushark, and Fawaz Alsolami. "Internet of Things (IoT) Security Intelligence: A Comprehensive Overview, Machine Learning Solutions and Research Directions." *Mobile Networks and Applications* 28, no. 1 (March 14, 2022): 296–312. https://doi.org/10.1007/s11036-022-01937-3.

Sellami, Bassem, Akram Hakiri, and Sadok Ben Yahia. "Deep Reinforcement Learning for Energy-Aware Task Offloading in Join SDN-Blockchain 5G Massive IoT Edge Network." *Future Generation Computer Systems* 137 (December 2022): 363–79. https://doi.org/10.1016/j.future.2022.07.024.

Sharma, Parjanay, Siddhant Jain, Shashank Gupta, and Vinay Chamola. "Role of Machine Learning and Deep Learning in Securing 5G-Driven Industrial IoT Applications." *Ad Hoc Networks* 123 (December 2021): 102685. https://doi.org/10.1016/j.adhoc.2021.102685.

Tang, Shensheng. "Performance Modeling and Optimization for a Fog-Based IoT Platform." *IoT* 4, no. 2 (June 2, 2023): 183–201. https://doi.org/10.3390/iot4020010.

Tariq, Usman, Irfan Ahmed, Ali Kashif Bashir, and Kamran Shaukat. "A Critical Cybersecurity Analysis and Future Research Directions for the Internet of Things: A Comprehensive Review." Sensors 23, no. 8 (April 19, 2023): 4117. https://doi.org/10.3390/s23084117.

Tariq, Usman, Irfan Ahmed, Muhammad Attique Khan, and Ali Kashif Bashir. "Fortifying IoT against Crimpling Cyber-Attacks: A Systematic Review." *Karbala International Journal of Modern Science* 9, no. 4 (October 14, 2023). https://doi.org/10.33640/2405-609x.3329.

Thakkar, Ankit, and Ritika Lohiya. "A Review on Machine Learning and Deep Learning Perspectives of IDS for IoT: Recent Updates, Security Issues, and Challenges." *Archives of Computational Methods in Engineering* 28, no. 4 (October 20, 2020): 3211–43. https://doi.org/10.1007/s11831-020-09496-0.

Wang, Changguang, Ziqiu Zhao, Fangwei Wang, and Qingru Li. "MSAAM: A Multiscale Adaptive Attention Module for IoT Malware Detection and Family Classification." Edited by Jinbo Xiong. *Security and Communication Networks* 2022 (June 21, 2022): 1–14. https://doi.org/10.1155/2022/2206917.

Wang, Jin, Chang Liu, Jiangpei Xu, Juan Wang, Shirong Hao, Wenzhe Yi, and Jing Zhong. "IoT-DeepSense: Behavioral Security Detection of IoT Devices Based on Firmware Virtualization and Deep Learning." Edited by Weizhi Meng. *Security and Communication Networks* 2022 (March 18, 2022): 1–17. https://doi.org/10.1155/2022/1443978.

Wang, Zhibo, Defang Liu, Yunan Sun, Xiaoyi Pang, Peng Sun, Feng Lin, John C. S. Lui, and Kui Ren. "A Survey on IoT-Enabled Home Automation Systems: Attacks and Defenses." *IEEE Communications Surveys & Tutorials* 24, no. 4 (2022): 2292–2328. https://doi.org/10.1109/comst.2022.3201557.

Wang, Zhendong, Hui Chen, Shuxin Yang, Xiao Luo, Dahai Li, and Junling Wang. "A Lightweight Intrusion Detection Method for IoT Based on Deep Learning and Dynamic Quantization." *PeerJ Computer Science* 9 (September 22, 2023): e1569. https://doi.org/10.7717/peerj-cs.1569.

Wei, Chongbo, Gaogang Xie, and Zulong Diao. "A Lightweight Deep Learning Framework for Botnet Detecting at the IoT Edge." *Computers & Security* 129 (June 2023): 103195. https://doi.org/10.1016/j.cose.2023.103195.

Wu, Chia-Yi, Tao Ban, Shin-Ming Cheng, Takeshi Takahashi, and Daisuke Inoue. "IoT Malware Classification Based on Reinterpreted Function-Call Graphs." *Computers & Security* 125 (February 2023): 103060. https://doi.org/10.1016/j.cose.2022.103060.

Wu, Yulei, Hong-Ning Dai, and Haina Tang. "Graph Neural Networks for Anomaly Detection in Industrial Internet of Things." *IEEE Internet of Things Journal* 9, no. 12 (June 15, 2022): 9214–31. https://doi.org/10.1109/jiot.2021.3094295.

Yang, Yi, Zixuan Pan, and Zhen Su. "Deep-Transfer Learning Framework in SDN for Gateway Ports Security." *Optik* 270 (November 2022): 170038. https://doi.org/10.1016/j.ijleo.2022.170038.

Yan, Lichao, Juan Hu, Yi Wang, Ning Zheng, and Jinhong Di. "A Communication Security Anti-Interference Decision Model Using Deep Learning in Intelligent Industrial IoT Environment." *Soft Computing* 26, no. 16 (March 14, 2022): 7993–8002. https://doi.org/10.1007/s00500-022-06901-7.

Yao, Haipeng, Pengcheng Gao, Jingjing Wang, Peiying Zhang, Chunxiao Jiang, and Zhu Han. "Capsule Network Assisted IoT Traffic Classification Mechanism for Smart Cities." *IEEE Internet of Things Journal* 6, no. 5 (October 2019): 7515–25. https://doi.org/10.1109/jiot.2019.2901348.

Yoon, Pil-Do, and Gyung-Ho Hwang. "Malicious Traffic Classification in a UNSW-NB15 Dataset by Using Tomeklinks and ClusBUS." *The Journal of Korean Institute of Communications and Information Sciences* 46, no. 11 (November 30, 2021): 1896–99. https://doi.org/10.7840/kics.2021.46.11.1896.

Yumlembam, Rahul, Biju Issac, Seibu Mary Jacob, and Longzhi Yang. "IoT-Based Android Malware Detection Using Graph Neural Network With Adversarial Defense." *IEEE Internet of Things Journal* 10, no. 10 (May 15, 2023): 8432–44. https://doi.org/10.1109/jiot.2022.3188583.

Yusuf GÜVEN, Ebu, and Zeynep GÜRKAŞ-AYDIN. "Mirai Botnet Attack Detection in Low-Scale Network Traffic." *Intelligent Automation & Soft Computing* 37, no. 1 (2023): 419–37. https://doi.org/10.32604/iasc.2023.038043.

Zhu, Jinting, Julian Jang-Jaccard, and Paul A. Watters. "Multi-Loss Siamese Neural Network With Batch Normalization Layer for Malware Detection." *IEEE Access* 8 (2020): 171542–50. https://doi.org/10.1109/access.2020.3024991.